Notice of Allowability	Application No.	Applicant(s)	
	10/533,120	SMEETS ET AL.	
	Examiner	Art Unit	
	MICHAEL PYZOCHA	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the After-Final amendment filed 08/02/2010 and the telephonic interview help 08/16/2010*.

2. ☒ The allowed claim(s) is/are *47-50,52 and 54-75*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 8/10/10
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *8/16/10* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Michael Pyzocha/
Primary Examiner, Art Unit 2437

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John Lastova (Reg. No. 33,149) on 08/16/2010.

The application has been amended as follows:

52. (Currently Amended) The electronic circuit according to claim 47, said electronic circuit ~~comprises~~ is configured to:

~~means for generating~~ generate, based on said stored secret and said configurational device- specific security data, said trigger data as a cryptographic representation of said configurational device-specific security data during configuration of said device;

~~means for outputting~~ output said cryptographic representation over an external circuit interface during configuration; and

~~means for internally re-generating~~ re-generate said device-specific security data during usage of said device provided that said additional input corresponds to said cryptographic representation.

54. (Currently Amended) The electronic circuit according to claim 52, wherein said ~~means for~~ internally re-generating said device-specific security data comprises ~~means for~~ generating a private key at least partly based on said stored secret, and said trigger data is generated as a cryptographic representation of said private key during configuration of said device.

55. (Currently Amended) The electronic circuit according to claim 47, further ~~comprising means for making~~ configured to make, during configuration of said device, said internally-confined, temporarily available instance of device-specific security data

available over the external circuit interface provided that a predetermined device access code is entered into the electronic circuit.

56. (Currently Amended) The electronic circuit according to claim 47, further ~~comprising means for disabling~~ configured to internal access to at least one of said stored secret and said device-specific security data unless a predetermined device access code is entered into the electronic circuit.

57. (Currently Amended) The electronic circuit according to claim 55, further ~~comprising~~ configured to:

~~means for authentication of~~ authenticate a manufacturer of said device;

~~means for providing~~ provide, during device manufacturing, said device access code to said device manufacturer in response to successful authentication.

58. (Currently Amended) The electronic circuit according to claim 47, wherein said electronic circuitry ~~comprises~~ is configured to:

~~means for performing~~ perform additional cryptographic processing based on said internally-confined, temporarily available instance of the device-specific security data and further external input data to generate further security data; and

~~means for performing~~ perform said security-related operation in response to said further security data.

63. (Currently Amended) The electronic circuit according to claim 62, further ~~comprising means for generating~~ configured to:

generate a public key corresponding to said private key during configuration of said device, and

~~means for outputting~~ output said public key over an external circuit interface.

64. (Currently Amended) The electronic circuit according to claim 62, further ~~comprising~~ configured to:

~~means for performing~~ perform shared key generation to generate a new shared key based on said generated private key and a public key of an intended communication partner; and

~~means for performing~~ perform cryptographic processing based on said new shared key.

Allowable Subject Matter

2. Claims 47-50, 52 and 54-75 are allowed.

3. The following is an examiner's statement of reasons for allowance: The prior art generally teaches manufacturing tamper resistant circuits and activating them/portions of them (i.e. secured data) by means of trigger data. However, the prior art does not disclose or render obvious "trigger data generating circuitry for, during configuration of the tamper-resistant electronic circuit, generating trigger data by cryptographically combining the random secret and device-specific security data that is different from the random secret and outputting the trigger data outside of the tamper-resistant electronic circuit" and "the temporarily available instance of the device-specific security data is only available when the externally received trigger data is received" together and in combination with the remaining claim limitations.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is

(571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 3:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Pyzocha/
Primary Examiner, Art Unit 2437